REMARKS/ARGUMENTS

The Office Action mailed April 4, 2008 has been carefully considered. Claims 49-57 are pending and newly added. Claims 1-48 are canceled without prejudice, waiver, or disclaimer. No new matter has been added.

Applicant respectfully submits that a majority of the subject matter of claims 49-52 and 54-56 was originally filed in claims 42-48 in the present patent application, and the originally filed claims 42-48 were examined in an Office Action mailed 16th May, 2006.

The 35 U.S.C. § 103 Rejection

Claims 1-36, 38-40, and 42-48 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Martinek et al. (WO 03/045519), referred to as Martinek, in view of Rackman (U.S. Patent No. 4,670,857). Applicant has canceled claims 1-36, 38-40, and 42-48. Accordingly, Applicants respectfully request that the Section 103 rejection of claims 1-36, 38-40, and 42-48 be withdrawn.

Applicant respectfully submits that neither Martinek nor Rackman, considered alone or in combination, describe or suggest "said controller being programmed to determine whether said first decrypted gaming data is identical to said second decrypted gaming data" as recited in claim 49, The first decrypted data is formed by decrypting first encrypted gaming data with an encryption key of the first gaming organization and the second decrypted data is formed by decrypting second encrypted gaming data with an encryption key of the second gaming organization. Rather, Martinek describes, on page 27, lines 30-33:

> One embodiment of the invention may use authentication programs that comprises the use of *hash functions* to calculate a reference hash value for selected data, which can later be compared to a hash value calculated from the same data or a copy of the data to ensure the data has not been altered.
> (Emphasis added)

Martinek further describes, on page 30, line 18 – page 31, line 2:

> In some embodiments of the invention, only the hash value needs to be encrypted with public key/private key encryption, greatly reducing the time needed to sign or verify large amounts of data. To verify the signature, the hash value is decrypted with the intended signer's public key and the decrypted reference hash value is compared to a newly-computed hash value of the same data. *If the reference hash value matches the newly-computed hash value, a degree of certainty exists that the signed data has not been altered since it was signed.* In some embodiments using digital signatures, the digital signature is that of a regulatory agency or other organization responsible for ensuring the integrity of data in computerized wagering game systems. *For example, the Nevada Gaming Regulations Commission may apply a signature to data used in such gaming systems, ensuring that they have approved the signed data.* Such an embodiment will be useful to ensure that game code executing in these systems has been approved and not altered since approval, and provides security both to the game operator or owner and to the regulatory commission. *In other embodiments, the digital signature is that of the game code manufacturer or designer, and ensures that the game code has not been altered from its original state since signing.*
>
> (Emphasis added).

Accordingly, Martinek describes a system that matches a reference hash value with a newly-computed hash value, where the reference hash value is generated by applying a plurality of hash functions to selected data, and the newly-computed hash value may be generated from the same data. Martinek also describes that the Nevada Gaming Regulations Commission may apply a digital signature to the data and in another embodiment, the game code manufacturer applies a digital signature to the data. Further, Rackman describes a transmitter that doubly encrypts a message with the transmitter's private key and a receiver's public key, and the receiver that doubly decrypts the message with the receiver's private key and the transmitter's public key (col. 5, line 67 – col. 6, line 3). A description of the match of the reference hash value with the newly-computed hash value in Martinek and a description of the double encryption and the

double decryption in Rackman does not describe or suggest the determination whether the first decrypted gaming data is identical to the second decrypted gaming data, where the first decrypted data is formed by decrypting first encrypted gaming data with an encryption key of the first gaming organization and the second decrypted data is formed by decrypting second encrypted gaming data with an encryption key of the second gaming organization. Hence, for at least the reasons set forth above, Applicants respectfully submit that claim 49 is patentable over Martinek in view of Rackman.

Claims 50-53 depend from independent claim 49. When the recitations of claims 50-53 are considered in combination with the recitations of claim 49, Applicant respectfully submits that claims 50-53 are also patentable over Martinek in view of Rackman.

Moreover, for at least the same reasons set forth above, neither Martinek nor Rackman, considered alone or in combination, describe or suggest "determining whether said first decrypted gaming data is identical to said second decrypted gaming data", where the first decrypted gaming data is formed by decrypting first encrypted gaming data with an encryption key of the first gaming organization, and the second decrypted gaming data is formed by decrypting second encrypted gaming data with an encryption key of the second gaming organization. Specifically, a description of the match of the reference hash value with the newly-computed hash value in Martinek and a description of the double encryption and the double decryption in Rackman does not describe or suggest determining whether the first decrypted gaming data is identical to the second decrypted gaming data. Hence, for at least the reasons set forth above, Applicants respectfully submit that claim 54 is patentable over Martinek in view of Rackman.

Claims 55-57 depend from independent claim 54. When the recitations of claims 55-57 are considered in combination with the recitations of claim 54, Applicant respectfully submits that claims 55-57 are also patentable over Martinek in view of Rackman.

In view of the foregoing, it is respectfully asserted that the pending claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited and Applicant respectfully requests that a timely Notice of Allowance be issued in this case. If,

in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

Applicant hereby petitions for a one-month extension of time from July 4, 2008 to August 4, 2008 to maintain the pendency of this case, and any required fee for such extension or any further fee required in connection with the filing of this Amendment is to be charged to Deposit Account No. 500388 (Order No. IGT1P551).

Respectfully submitted,

/David P. Olynick/

David P. Olynick
Reg. No. 48,615
Weaver Austin Villeneuve & Samspon LLP
P.O.Box 70250
Oakland, CA 94612-0250